Microsoft Azure Security Technologies

Duration: 4 Days

Course Description:

This course provides IT Security Professionals with the knowledge and skills needed to implement security controls, maintain an organization's security posture, and identify and remediate security vulnerabilities. This course includes security for identity and access, platform protection, data and applications, and security operations.

Intended Audience:

This course is for Azure Security Engineers who are planning to take the associated certification exam, or who are performing security tasks in their day-to-day job. This course would also be helpful to an engineer that wants to specialize in providing security for Azure-based digital platforms and play an integral role in protecting an organization's data.

Course Outline:

Manage identities in Microsoft Entra ID

- Introduction
- What is Microsoft Entra ID?
- Secure users in Microsoft Entra ID
- Secure groups in Microsoft Entra ID
- Recommend when to use external identities
- Secure external identities
- Implement Microsoft Entra Identity protection

Manage authentication by using Microsoft Entra ID

- Introduction
- What is Microsoft Entra authentication?
- Implement multifactor authentication (MFA)
- Implement password less authentication
- Implement password protection
- Implement single sign-on (SSO)
- Integrate single sign-on (SSO) and identity providers
- Introduction to Microsoft Entra Verified ID
- Configure Microsoft Entra Verified ID
- Recommend and enforce modern authentication protocols

Manage authorization by using Microsoft Entra ID

- Introduction
- Configure Azure role permissions for management groups, subscriptions, resource groups, and resources
- Assign built-in roles in Microsoft Entra ID
- Assign built-in roles in Azure
- Create and assign a custom role in Microsoft Entra ID
- Implement and manage Microsoft Entra Permissions Management
- Configure Microsoft Entra Privileged Identity Management
- Enable and monitor database audit
- Identify use cases for the Microsoft Purview governance portal
- Implement data classification of sensitive information by using the Microsoft Purview governance portal
- Plan and implement dynamic mask
- Implement transparent data encryption
- Recommend when to use Azure SQL Database Always Encrypted
- Microsoft Entra ID Governance
- Entitlement management
- Access reviews
- Identity lifecycle management
- Lifecycle workflows
- Delegation and roles in entitlement management
- Configure role management and access reviews by using Microsoft Entra ID Governance
- Implement Conditional Access policies

Plan, implement, and manage governance for security

- Introduction
- Create, assign, and interpret security policies and initiatives in Azure Policy
- Configure security settings by using Azure Blueprint
- Deploy secure infrastructures by using a landing zone
- Create and configure an Azure Key Vault
- Recommend when to use a dedicated Hardware Security Module (HSM)
- Configure access to Key Vault, including vault access policies and Azure Role Based Access Control
- Manage certificates, secrets, and keys
- Configure key rotation
- Configure backup and recovery of certificates, secrets, and keys

Plan and implement security for public access to Azure resources

- Introduction
- Plan and implement Transport Layer Security (TLS) to applications, including Azure App Service and API Management
- Plan, implement, and manage an Azure Firewall, Azure Firewall Manager and firewall policies
- Plan and implement an Azure Application Gateway
- Plan and implement an Azure Front Door, including Content Delivery Network (CDN)
- Plan and implement a Web Application Firewall (WAF)
- Recommend when to use Azure DDoS Protection Standard

Plan and implement advanced security for compute

- Introduction
- Plan and implement remote access to public endpoints, Azure Bastion and just-in-time (JIT) virtual machine (VM) access
- Configure network isolation for Azure Kubernetes Service (AKS)
- Secure and monitor AKS
- Configure authentication for AKS
- Configure security for Azure Container Instances (ACIs)
- Configure security for Azure Container Apps (ACAs)
- Manage access to Azure Container Registry (ACR)
- Configure disk encryption, Azure Disk Encryption (ADE), encryption as host, and confidential disk encryption
- Recommend security configurations for Azure API Management

Plan and implement security for storage

- Introduction
- Configure access control for storage accounts
- Manage life cycle for storage account access keys
- Select and configure an appropriate method for access to Azure Files

- Select and configure an appropriate method for access to Azure Blob Storage
- Select and configure an appropriate method for access to Azure Tables
- Select and configure an appropriate method for access to Azure Queues
- Select and configure appropriate methods for protecting against data security threats, including soft delete, backups, versioning, and immutable storage
- Configure Bring your own key (BYOK)
- Enable double encryption at the Azure Storage infrastructure level

Manage security posture by using Microsoft Defender for Cloud

- Introduction
- Implement Microsoft Defender for Cloud
- Identify and remediate security risks by using the Microsoft Defender for Cloud Secure Score and Inventory
- Assess compliance against security frameworks and Microsoft Defender for Cloud
- Add industry and regulatory standards to Microsoft Defender for Cloud
- Add custom initiatives to Microsoft Defender for Cloud
- Connect hybrid cloud and multicloud environments to Microsoft Defender for Cloud
- Identify and monitor external assets by using Microsoft Defender External Attack Surface Management

Configure and manage threat protection by using Microsoft Defender for Cloud

- Introduction
- Enable workload protection services in Microsoft Defender for Cloud, including Microsoft Defender for Storage, Databases, Containers, App Service, Key Vault, Resource Manager, and DNS
- Configure Microsoft Defender for Servers
- Configure Microsoft Defender for Azure SQL Database
- Manage and respond to security alerts in Microsoft Defender for Cloud
- Configure workflow automation by using Microsoft Defender for Cloud
- Evaluate vulnerability scans from Microsoft Defender for Server

Manage application access in Microsoft Entra ID

- Introduction
- Manage access to enterprise applications in Microsoft Entra ID, including OAuth permission grants
- Manage app registrations in Microsoft Entra ID
- Configure app registration permission scopes
- Manage app registration permission consent
- Manage and use service principals
- Manage managed identities for Azure resources
- Recommend when to use and configure a Microsoft Entra Application Proxy, including authentication

Plan and implement security for virtual networks

- Introduction
- Plan and implement Network Security Groups (NSGs) and Application Security Groups (ASGs)
- Plan and implement User-Defined Routes (UDRs)
- Plan and implement Virtual Network peering or gateway
- Plan and implement Virtual Wide Area Network, including secured virtual hub
- Secure VPN connectivity, including point-to-site and site-to-site
- Azure ExpressRoute
- Implement encryption over ExpressRoute
- Configure firewall settings on PaaS resources
- Monitor network security by using Network Watcher, including network security groups

Plan and implement security for private access to Azure resources

- Introduction
- Plan and implement virtual network Service Endpoints
- Plan and implement Private Endpoints
- Plan and implement Private Link services
- Plan and implement network integration for Azure App Service and Azure Functions
- Plan and implement network security configurations for an App Service Environment (ASE)
- Plan and implement network security configurations for an Azure SQL Managed Instance

Configure and manage security monitoring and automation solutions

- Introduction
- Monitor security events by using Azure Monitor
- Configure data connectors in Microsoft Sentinel
- Create and customize analytics rules in Microsoft Sentinel
- Configure automation in Microsoft Sentinel

Plan and implement security for Azure SQL Database and Azure SQL Managed Instance

- Introduction
- Enable database authentication by using Microsoft Entra ID